

(19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

(11) N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 770 316

(21) N° d'enregistrement national :

98 00428

(51) Int Cl⁶ : G 06 K 7/08, G 06 K 19/073

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 16.01.98.

(71) Demandeur(s) : MORENO ROLAND — FR.

(30) Priorité : 24.10.97 FR 09713345.

(72) Inventeur(s) : MORENO ROLAND.

(43) Date de mise à la disposition du public de la
demande : 30.04.99 Bulletin 99/17.

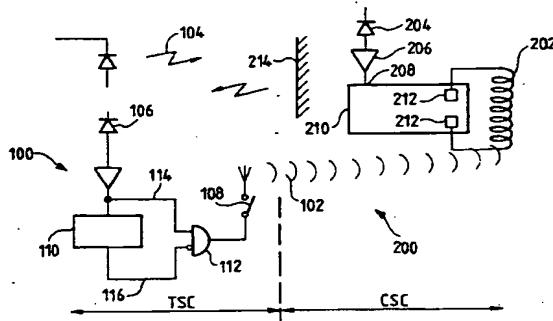
(73) Titulaire(s) :

(56) Liste des documents cités dans le rapport de
recherche préliminaire : Se reporter à la fin du
présent fascicule

(74) Mandataire(s) : CABINET BARDEHLE PAGENBERG
ET PARTNER.

(54) SYSTEME POUR LA COMMUNICATION SECURISEE SANS CONTACT ENTRE UN TERMINAL ET UN OBJET
PORTATIF TEL QU'UNE CARTE A PUCE.

(57) Le terminal et la carte comportent chacun des moyens
émetteurs-récepteurs de champ électromagnétique et la
carte comporte une puce (210) avec des circuits de traite-
ment et une mémoire inscriptible sur commande du termi-
nal. Selon l'invention, la carte comporte des moyens de
validation conditionnant au moins une étape du déroule-
ment de la communication à une action pré-déterminée ex-
térieure de confirmation exercée par le porteur de la carte.
Les moyens de validation comportent, dans la carte, des
moyens récepteurs de lumière coopérant avec les circuits
électroniques de traitement numérique et avec la mémoire.



L'invention concerne la communication sans contact entre deux organes distants tels qu'un terminal fixe et un objet portatif électronique indépendant détenu par un utilisateur.

De tels systèmes d'échange de données sans contact (c'est-à-dire sans contact galvanique) sont bien connus et, parmi les applications de cette technique, on trouve — de façon non limitative : le contrôle d'accès physique, par exemple pour l'accès à un local protégé ou dont l'accès est restreint à certaines personnes devant au préalable s'identifier ; le contrôle d'accès logique, par exemple à une fonction informatique ; le dé-
cryptage de données, etc. ; ainsi que les transactions monétaires telles que les applications du type "porte-monnaie électronique", les applications de péage ou de paiement, etc.

À cet égard, bien que dans la description détaillée on fasse souvent référence à une transaction de paiement, cette application n'est nullement limitative et l'invention peut être mise en œuvre pour toute application, impliquant un échange d'informations sans contact, telle que celles que l'on vient de citer.

L'utilisateur est pourvu d'un objet portatif par exemple du type "carte sans contact" ou "badge sans contact", que l'on appellera ci-après simplement "carte" — le terme de "carte" n'étant cependant choisi que par commodité et sans aucun caractère limitatif, l'invention s'appliquant à tout type d'objet portatif électronique tel que badge, bague, bracelet, clef, pendentif, etc. susceptible d'échanger des informations avec un terminal sans contact (ci-après "terminal") en approchant la carte de ce dernier de manière à permettre un couplage non galvanique entre ces deux organes.

L'échange d'informations consécutif à ce couplage est opéré en modulant un champ électromagnétique qui peut être soit un champ où la composante électrique est dominante (dans le domaine des radiofréquences, hyperfréquences ou même fréquences lumineuses) ou bien dans laquelle la composante magnétique est prépondérante, le couplage étant alors opéré en faisant varier un champ magnétique produit par une bobine d'induction, technique connue sous le nom de "procédé par induction". La carte utilisée dans le cadre de cette dernière technique, quel que soit le procédé mis en œuvre, peut être du type "actif", c'est-à-

dire comportant une pile d'alimentation incorporée, ou bien "passif", c'est-à-dire télalimentée par de l'énergie émise par le terminal, notamment de l'énergie magnétique, ce qui fait souvent préférer le procédé par induction.

5 L'invention vise la protection contre un certain risque de fraude et de malveillance auquel le type de système à communication sans contact par champ électromagnétique pourrait être exposé.

Plus précisément, ce type de système est vulnérable au "vol à la tire électronique", où un fraudeur "pickpocket électronique" approche 10 de la carte, à l'insu de son porteur, un terminal portable contrefait pour établir frauduleusement un lien de communication avec la carte et, par exemple dans le cas d'un porte-monnaie électronique, prélever indûment des unités monétaires dans la mémoire de la carte.

Certes, dans de telles applications, il est souvent prévu des sécurités par codage ou cryptage, mais ces sécurités sont souvent limitées 15 dans leurs performances en raison de la place mémoire importante qu'elles requièrent dans la carte et du prolongement des temps de communication qu'elles peuvent entraîner.

Il apparaît donc nécessaire de prévoir des moyens permettant 20 d'empêcher de manière simple une telle fraude à l'insu de l'utilisateur.

L'invention propose à cet effet un système pour la communication sans contact entre un terminal et un objet portatif tel qu'une carte, le terminal et la carte comportant chacun des moyens émetteurs-récepteurs de champ électromagnétique et la carte comportant une puce avec 25 des circuits de traitement et une mémoire inscriptible sur commande du terminal, caractérisé en ce que la carte comporte des moyens de validation, conditionnant au moins une étape du déroulement de la communication à une action prédéterminée extérieure de confirmation exercée avec cette carte par le porteur de la carte, ces moyens de validation comportant, dans la carte, des moyens récepteurs de lumière co-opérant avec les circuits électroniques de traitement numérique et avec 30 la mémoire.

Avantageusement, selon divers modes de réalisations ou variantes de l'invention :

35 — l'action prédéterminée de confirmation est l'exposition de la carte à

l'éclairement ambiant ;

- la mémoire contient une donnée formant indicateur d'activation ou d'inhibition des moyens de validation indiquant si, respectivement, ladite étape du déroulement de la communication doit ou non être conditionnée à ladite action prédeterminée extérieure de confirmation ;
- cet indicateur d'activation ou d'inhibition est une donnée statique prédeterminée, qui peut être irréversiblement prédeterminée, ou bien modifiable dynamiquement par une borne lors du déroulement d'une communication ;
- l'étape conditionnelle du déroulement de la communication est l'activation de l'écriture et/ou de la lecture de la mémoire de la carte.

◊

15

On va maintenant décrire diverses mises en œuvre de l'invention, en référence aux dessins annexés.

La figure 1 est une vue générale schématique du système de l'invention.

20 La figure 2 illustre de façon plus précise l'échange des signaux entre carte et terminal.

La figure 3 est un organigramme explicitant le déroulement des diverses étapes de communication entre carte et terminal.

La figure 4 illustre un mode de réalisation de la puce de la carte.

25 La figure 5 est un premier perfectionnement du mode de réalisation de la figure 4.

La figure 6 est un deuxième perfectionnement du mode de réalisation de la figure 4.

30 La figure 7 montre la carte pourvue de moyens de détection d'action digitale.

La figure 8 montre la carte pourvue de moyens de détection d'action par contrainte de la carte.

La figure 9 montre la carte pourvue de moyens de détection de type cible magnétique antivol.

35 La figure 10 montre la carte pourvue de moyens de détection de

type cibles magnétiques codées.

La figure 11 illustre la manière dont sont codées les cibles de la figure 10.

La figure 12 montre le système avec le terminal pourvu de moyens 5 de détection de détection de la carte par occultation.

La figure 13 montre le système avec le terminal pourvu de moyens télémétriques de détection de la carte.

La figure 14 est un chronogramme de divers signaux relevés sur le montage de la figure 13.

10 La figure 15 montre une première configuration des moyens émetteurs-récepteurs de lumière du terminal.

La figure 16 montre une deuxième configuration des moyens émetteurs-récepteurs de lumière du terminal.

15 La figure 17 montre une troisième configuration des moyens émetteurs-récepteurs de lumière du terminal.

La figure 18 est une vue d'une puce monolithique intégrant les moyens récepteurs de lumière.

La figure 19 montre une implantation possible de la puce de la figure 18 dans la carte du système.

20 La figure 20 montre une carte pourvue de moyens réflecteurs de lumière.

La figure 21 illustre la mise en œuvre à reconnaissance mutuelle du système de l'invention.

25 La figure 22 illustre une logique de commande d'une carte à inhibition de lecture et/ou écriture en fonction de la présence d'une lumière extérieure.

La figure 23 est une variante de la figure 22, permettant une invalidation conditionnelle du circuit inhibiteur.

30 La figure 24 est une variante de la figure 22, permettant une acquisition conditionnelle des consignes.

La figure 25 illustre de façon schématique un moyen de compensation automatique du fonctionnement du circuit de la carte selon le niveau de l'éclairage extérieur.

35 La figure 26 illustre une configuration particulière de réalisation de l'organe photoélectrique de la carte, vue de dessus.

La figure 27 est une coupe selon A-A de la figure 26.

La figure 28 est une coupe selon B-B de la figure 26.

La figure 29 illustre une autre configuration particulière de réalisation de l'organe photoélectrique de la carte, vue de dessus.

5

◊

Selon un premier aspect de l'invention, pour éviter les risques de "vol à la tire électronique" il est prévu qu'au moins une partie critique 10 de la communication entre la carte et le terminal soit rendue conditionnelle sur une action volontaire de la part de l'utilisateur. De façon particulièrement avantageuse, cette action volontaire peut être captée par la détection d'une lumière, la fonction de communication étant rendue conditionnelle sur la présence (ou l'absence) de cette détection de la 15 lumière.

Le terminal peut ainsi comporter un détecteur de lumière sensible à la réflexion de lumière par la carte, l'action volontaire consistant à sortir la carte, normalement rangée dans un étui ou une poche, et à la présenter dans la lumière au terminal. Le terminal peut détecter la lumière ambiante réfléchie par la carte et débloquer la communication. 20 Pour distinguer la lumière reçue par le terminal de la lumière ambiante, la lumière peut incorporer des caractéristiques particulières, par exemple on peut prévoir que la réflexion par la carte transmette sélectivement certaines combinaisons caractéristiques de couleurs (ou de 25 longueurs d'onde si la lumière n'est pas une lumière visible).

Dans un mode réalisation particulièrement avantageux, c'est un faisceau lumineux émis par le terminal (on verra plus bas que ce même faisceau peut éventuellement servir à désactiver et réactiver le champ électromagnétique) qui est réfléchi par la carte et détecté par le terminal, ce dernier pouvant alors moduler le faisceau pour l'encoder, ce qui permet un décodage simple du faisceau réfléchi pour le reconnaître et le distinguer de la lumière ambiante, mais aussi de faisceaux en provenance d'autres terminaux proches.

La modulation du faisceau peut être une modulation de fréquence, 35 de phase, d'amplitude ou par impulsions, par exemple.

La détection de lumière peut être opérée dans la carte, l'action volontaire consistant à sortir la carte pour la présenter au terminal ; dans ce cas, la carte peut comporter un détecteur de lumière ambiante, un élément photosensible tel qu'une photodiode, un phototransistor ou un élément photovoltaïque, par exemple.

5 Dans un mode de réalisation préférentiel, que l'on exposera plus bas en détail, la carte incorpore une surface réfléchissante et un détecteur d'un faisceau émis par le terminal, ce dernier comportant un détecteur du faisceau réfléchi par la carte.

10 Le détecteur de la carte peut alors servir pour ranimer la carte (en état de veille à basse consommation en l'absence du faisceau), tandis que l'encodage du faisceau peut incorporer un contenu informationnel (un code spécifique d'habilitation par exemple) auquel la carte est sensible. La détection au terminal du faisceau réfléchi peut en outre servir, 15 comme on l'exposera plus bas, à augmenter la puissance du champ électromagnétique produit par ce dernier (ou à en déclencher l'émission), comme on le décrira plus bas.

20 Ces divers modes de réalisation se prêtent au déclenchement automatique ou semi-automatique de l'initialisation de la transaction par la détection de l'entrée de la carte dans la zone du champ émis ou à émettre par le terminal.

25 En variante, l'initialisation (et/ou la communication tout entière avec le terminal) peut être déclenchée par un actionnement manuel de la carte. En particulier, la carte peut être munie d'un commutateur dont l'actionnement déclenche le déverrouillage de la carte et l'engagement de la transaction. Au lieu de prévoir un commutateur en forme de bouton, avec les problèmes classiques d'implantation et de fiabilité des contacts, dans une réalisation préférée de carte à double communication contacts (selon ISO 7816)/sans contact, la fonction du commutateur 30 est assurée par les plages de contact galvaniques de la carte conçues pour assurer la communication avec un terminal à contacts : en mode de communication sans contact, le microprocesseur de la carte, téléalimenté par le champ émis par le terminal, applique une tension entre deux ou plusieurs des plages de contact et détecte des courants faibles 35 qui passent entre les plages lorsque l'utilisateur appuie son doigt sur

ces dernières.

Dans une autre variante, la carte peut comporter un élément sensible à une manipulation de la carte par l'utilisateur, par exemple grâce à un élément de type jauge de contrainte sensible à la flexion de la carte, 5 ou encore un élément par exemple piézoélectrique sensible à la pression exercée sur une zone particulière de la carte.

Un autre aspect de l'invention, qui peut tout à fait se combiner au précédent, vise à réduire ou interrompre les émissions de champ électromagnétique dans des périodes où la pleine puissance n'est pas requise en continu, l'émission du champ électromagnétique pouvant être 10 réactivée lorsqu'une carte est présente ou susceptible de se présenter.

Non seulement on réduit les risques inhérents aux émissions de champ électromagnétique, mais on peut aussi obtenir une économie de consommation d'énergie dans la génération du champ.

15 Le terminal peut comporter des moyens de détection de l'approche ou de la présence d'un utilisateur pour réactiver l'émission du champ. Dans un mode de réalisation préféré, notamment pour le contrôle d'accès informatique ou logique, mais aussi pour d'autres applications, les moyens de détection comprennent un détecteur de lumière ambiante 20 (une cellule photoélectrique par exemple) qui est occultée par l'approche de la carte ou de la main ou du poignet de l'utilisateur tenant la carte.

Dans un autre mode de réalisation, plutôt adapté au contrôle d'accès physique, les moyens de détection peuvent inclure un faisceau lumineux qui traverse le passage d'accès jusqu'à une cellule photoélectrique 25 en vis-à-vis, et qui est interrompu par l'approche de l'utilisateur.

Dans une variante, l'approche de l'utilisateur peut être détectée par un détecteur de poids (par exemple plus de 20 kg) situé sous le passage d'accès, par exemple.

30 Dans encore un autre mode de réalisation, le terminal peut être réactivé lorsque des moyens de contrôle de passage sont libérés, lors de l'ouverture de la porte d'un bus, par exemple.

Au lieu de s'éteindre complètement, le terminal peut fonctionner à 35 champ réduit pendant la période quiescente, champ juste suffisant pour permettre la détection de l'approche d'une carte, puis se réactiver à

puissance plus forte pour l'échange de données avec la carte. Le terminal ne fonctionne pas nécessairement en continu pendant la période quiescente et peut émettre une courte interrogation répétitive pendant cette période (par exemple pendant 100 ms toutes les secondes), à plein 5 champ ou à champ réduit.

Une autre façon de commander la réactivation du terminal est de la déclencher en fonction d'un signal d'initialisation transmis au terminal par la carte. Dans le cas d'une carte autoalimentée (par pile interne, par exemple), le signal d'initialisation peut être engendré et émis 10 par la carte. Dans le cas d'une carte sans alimentation interne, on peut prévoir de basculer la carte vers un état de fonctionnement à consommation d'énergie réduite, en activant seulement les parties des circuits directement nécessaires pour l'initialisation (les couches de communication et un circuit de modulation avec les données d'identification et 15 un récepteur en veille).

Le terminal émet alors à l'état quiescent un champ électromagnétique à puissance réduite, juste suffisant pour activer la carte en son état de fonctionnement réduite.

Dans tous ces cas, les moyens de détection peuvent inclure un récepteur sensible au signal d'initialisation, qui peut être le même que 20 celui qui reçoit les données de communication en provenance de la carte en fonctionnement réactivé.

Dans d'autres variantes, au lieu d'utiliser les mêmes voies de communication pour la téléalimentation et/ou la transmission de données 25 que pour la transmission d'un signal d'initialisation, on peut prévoir une voie de communication différente pour l'initialisation du terminal. Ainsi, la carte peut inclure un ou plusieurs anneaux en matière magnétique, du ferrite par exemple, ce qui permet de détecter la présence de la carte avec un champ électromagnétique (émis par le terminal) encore plus faible. 30

La voie de communication pour l'initialisation peut même être complètement différente ; dans un mode de réalisation préféré, on prévoit une surface réfléchissante sur la carte et l'émission par le terminal d'un faisceau lumineux (pas nécessairement dans les longueurs d'onde de la lumière visible) dont la réflexion par la carte est détectée au terminal 35

par une cellule. Dans ce mode de réalisation, on s'affranchit pour l'initialisation de la nécessité de téléalimentation même d'une carte qui n'est pas autoalimentée. Afin de s'assurer une certaine latitude dans l'angle de présentation de la carte qui garantisse que la réflexion du faisceau arrive à la cellule sur le terminal, la surface réfléchissante est de préférence catadioptrique, c'est-à-dire à la fois réflectrice et réfractive, par exemple en forme d'un réseau de prismes transparents ou translucides, ou à billes rétroréfléchissantes, renvoyant le faisceau incident sur un angle solide nettement plus large que l'angle du faisceau lui-même.

On va maintenant décrire divers exemples particuliers de réalisation de l'invention, en référence aux dessins annexés.

Sur ces figures, la référence 100 désigne de façon générale le terminal sans contact ou TSC, et la référence 200 la carte sans contact ou CSC, le terme de "carte" utilisé n'étant, comme précisé plus haut, bien entendu aucunement limitatif.

Sur la figure 1, le terminal 100 est conçu pour émettre un champ électromagnétique 102, par exemple à 13,57 MHz, lequel permet l'activation d'une carte 200, ainsi qu'un rayon lumineux 104 en direction de la carte. La carte 200 capte l'énergie électromagnétique au moyen d'un bobinage 202 d'un circuit accordé sur la fréquence du champ 102, est extrait de ce champ l'énergie nécessaire à son fonctionnement pour :

- l'établissement de l'alimentation interne V_{cc} et la "remise à zéro à froid" associée à la mise sous tension des circuits de la puce de la carte, et
- le démarrage du microprocesseur ou des circuits électroniques dans le cas d'une puce de type "logique câblée".

Aussitôt débute la transaction sans contact : par exemple, pour une transaction de paiement sans contact, échange des caractères et des commandes préliminaires à la transaction proprement dite telles que : date, numéro de série et de lot, informations à caractère bancaire, validité, etc.

Préalablement au paiement, un élément photodéTECTeur 204 est interrogé pour détecter la présence éventuelle du rayon lumineux 104 attendu du terminal ; sur présence à ses bornes d'un signal électrique

prédéterminé, la transaction est autorisée à s'exécuter. Si le signal n'est pas observé dans les conditions prévues (par exemple, au bout de m millisecondes ou bien j itérations d'une boucle logicielle) l'écriture en mémoire est refusée, éventuellement jusqu'à mise hors tension de la 5 puce, c'est-à-dire jusqu'à sortie du champ. Le terminal ne recevant pas de la carte confirmation de l'écriture attendue, il refuse par conséquent la transaction.

Ainsi, un "pickpocket électronique" muni d'une antenne, par exemple un bobinage dissimulé dans un gant et relié à un boîtier simulateur 10 de terminal porté dans une poche ou dans un sac, ne peut actionner efficacement la carte à l'insu de l'utilisateur : même si le champ électromagnétique 102 est correctement émis par l'antenne du pickpocket, et que la carte est par conséquent correctement alimentée et initialisée, cette dernière ne saurait, hors la volonté de son porteur, recevoir le 15 faisceau lumineux nécessaire à l'accomplissement de la transaction, et donc de l'écriture puis du compte rendu qui doit en être fait au terminal.

Plus précisément, comme illustré figure 2, l'élément photodéTECTeur 204 est relié, via un circuit amplificateur et démodulateur 206, à une 20 entrée 208 de la puce 210 elle-même reliée, via les plots 212, à l'antenne (bobinage) 202, le tout étant monté sur une carte 200 portant un organe photoréfléchissant 214 tel que catadioptre, cataphote, bande 25 d'adhésif rétroréfléchissant, etc. C'est grâce à ce moyen photoréfléchissant prévu sur la carte que le rayon 104 émis par le terminal retourne à la photodiode 106 de ce même terminal, ce qui entraîne le déclenchement, schématisé par l'interrupteur 108, de l'émission du champ électromagnétique 102 nécessaire à l'opération de transaction sans contact, ceci via les circuits 110 du terminal. A tout instant, grâce à la porte ET 30 112, le champ électromagnétique peut être interrompu par l'un ou l'autre des deux signaux RAYON RECU = 'FAUX' (signal 114) ou FIN DE TRANSACTION = 'VRAI' (signal 116).

L'organigramme de la figure 3 explicite la séquence de fonctionnement du système terminal-carte.

Sur réception du champ électromagnétique émis par le terminal 35 (étape 300), la carte extrait l'énergie nécessaire à son fonctionnement

(établissement de l'alimentation interne V_{cc} , étape 302), puis à son initialisation :

- signal de remise à zéro automatique (étape 304),
- démarrage du microprocesseur ou des circuits électroniques dans le 5 cas d'une puce de type à logique câblée (étape 306).

Aussitôt débute le protocole d'échange de données sans contact (étape 308) : échange des caractères et commandes préliminaires à la transaction proprement dite (date, numéro de lot, validité, etc.).

À partir de ce moment la carte peut être débitée sur simple activation 10 d'un signal d'écriture en mémoire permettant l'inscription du montant du débit.

Dans un mode de réalisation préférentiel, on impose une condition pour que l'écriture intervienne dans la carte, à savoir l'établissement 15 d'un bit "transaction autorisée" (étape 310), par des moyens que l'on expliquera ci-dessous en référence à la figure 5. La boucle d'attente 312 permet que, dans le mouvement de présentation de la carte au terminal qui ne dure que quelques fractions de seconde, intervienne un positionnement correct de l'élément photodétecteur 204 vis-à-vis du rayon lumineux 104 pendant quelques millisecondes. Une fois la transaction 20 autorisée, on peut alors écrire le débit proprement dit, du montant x prévu, par exemple 25 francs. Après cela, la suite et la fin du processus de paiement peuvent avoir lieu (étape 312) la carte pouvant en particulier rendre compte au terminal par un dernier message de l'accomplissement d'une transaction complète.

25 On notera que, au cas où la carte s'éloigne du terminal au point de ne plus pouvoir poursuivre correctement l'échange des signaux avec le terminal, elle retourne immédiatement à son état inerte antérieur à l'entrée en communication et le déroulement de l'organigramme de la figure s'interrompt de ce fait, permettant le retour à l'état initial également côté terminal.

30 La figure 4 illustre de façon schématique, un mode de réalisation de l'invention qui ne nécessite pas de modification du logiciel de pilotage de la puce (dans le cas d'une carte à microprocesseur), ni d'un quelconque agencement logique préexistant d'une carte à logique câblée. Ceci 35 présente un grand intérêt, en particulier dans le cas de puces dont la

conception est déjà figée notamment pour répondre à des normes internationales ou autres contraintes pesant sur la définition spécifique d'un système de paiement rapide par exemple.

5 Pour ce faire, on peut organiser la puce 210 de manière qu'elle possède :

- une entrée spécifique EEPROMWE* autorisant l'écriture dans la mémoire EEPROM par application d'un signal 218 à l'état bas et,
- une sortie spécifique O₂ 220 qui produit un signal VRV* ("volonté reçue et vérifiée") qui devient vrai (à l'état bas) après réception et 10 vérification du signal impliquant la volonté de l'usager.

Les autres composants représentés sont :
— le bobinage 202, relié à l'entrée I₁ et la sortie O₁ de la puce,
— l'entrée spécifique I₂ recevant par le conducteur 221 le signal CV ("confirmation de volonté") détecté par exemple par la photodiode 15 ou par divers autres moyens qui seront exposés plus loin en référence aux figures 7 et suivantes,

20 — une entrée RAMWE* d'écriture en RAM qui, dans le cas présent, est reliée par la connexion 222 au potentiel de la masse de manière à rendre possible à tout moment une écriture en RAM des compteurs, bascules, registres, piles, etc. En revanche, l'écriture en EEPROM qui, seule, permet une transaction utile, dépend matériellement — et seulement matériellement — de la vérité du signal VRV* en 220, sans qu'il soit besoin de modifier en quoi que ce soit l'agencement interne, logique ou logiciel, de la puce 210.

25 Les seules contraintes associées à cette variante de réalisation consistent à :

- isoler sur la puce le "fil" (métallisation de la puce) général de commande d'écriture en EEPROM, et
- relier à celui-ci la sortie stable (elle-même issue d'un registre ou 30 d'une bascule) indiquant la réception et la vérification du signal fournissant une indication de la volonté de l'usager, éventuellement avec interposition de moyens de chiffrement/déchiffrement 224 pour accroître la sécurité intrinsèque des informations échangées.

35 Les figures 5 et 6 illustrent des perfectionnements du mode de mise

en œuvre que l'on vient de décrire, en prévoyant une discrimination supplémentaire opérée par la carte sur les caractéristiques physiques du rayon lumineux émis par le terminal (figure 5) et/ou un contenu informationnel véhiculé par ce même rayon lumineux (figure 6).

5 Sur la figure 5, le rayon lumineux 104, reçu par le photodétecteur 204 et amplifié en 206, est appliqué à un circuit 226 de démodulation et décodage susceptible d'extraire des informations représentatives de la fréquence F, de la phase ϕ et du motif ou "pattern" P propres à l'émission lumineuse 104. Ces paramètres sont comparés à des valeurs attendues 10 conservées dans la mémoire 228 de la puce et appliquées sur une entrée de référence 230 du circuit 226. La conformité de tous ces paramètres est détectée par la porte 230 et transmise via une bascule 232 à la porte 234 qui, en pilotant l'entrée d'écriture WRITE de la mémoire 228, autorise l'inscription dans celle-ci du montant x de la transaction.

15 En variante ou en complément de cette discrimination supplémentaire par les caractéristiques de modulation du faisceau lumineux, caractéristiques conservées dans la mémoire de la carte pour permettre la reconnaissance, il est possible d'opérer une discrimination sur des paramètres informationnels transmis par le faisceau modulé 104 et proches 20 à la carte (parité, caractères prédéterminés, jusques et y compris le propre numéro de série de la carte, ou encore numéro d'immatriculation ou coordonnées bancaires, notamment dans certaines variantes de porte-monnaie électronique).

25 Dans ce dernier cas, après démodulation et décodage par le circuit 206, un organe de comparaison 236 détermine la conformité de l'information reçue via le rayon lumineux (et donc répercute par le terminal, ce dernier l'ayant lui-même reçue de la mémoire de la carte) avec le numéro directement extrait de la mémoire 228, le cas échéant après déchiffrement par le circuit 238.

30 Les agencements que l'on vient de décrire sont particulièrement avantageux lorsqu'il y a risque de "collision" entre des informations émises et reçues par une pluralité de cartes simultanément présentes dans le champ (hertzien ou lumineux) du terminal.

35 En variante, l'exploitation du signal délivré par l'élément photodétecteur de la carte peut intervenir en début de processus, après extrac-

tion de l'alimentation puis remise à zéro à froid et avant toute émission par la carte, c'est-à-dire entre les étapes 306 et 308 de l'organigramme de la figure 3. De cette façon, aucune information provenant de la carte ne pourra être captée par qui que ce soit sans qu'un geste volontaire 5 spécifique n'ait été fait par le porteur de la carte, à savoir sortir la carte de sa poche ou de son portefeuille et placer celle-ci dans le champ du rayonnement lumineux.

On va maintenant décrire, en référence aux figures 7 et suivantes, diverses variantes de réalisation du moyen par lequel l'usager peut 10 exprimer sa volonté d'effectuer la transaction.

Ainsi, dans une variante "digitale" illustrée sur la figure 7, dans le cas d'une carte mixte permettant indifféremment d'effectuer des transactions sans contact ou via des contacts (typiquement, des contacts à la norme ISO 7816), la puce 210 comporte un circuit 240 de détection relié 15 par la série de conducteurs 242 aux différentes plages de contact 244 de la carte. Ces contacts 244 servent, en mode "à contacts" à fournir à la puce 210 à la fois les signaux d'échange de données et la tension d'alimentation. En mode "sans contact", c'est bien entendu la bobine 202 qui assure ces fonctions. Le circuit 240 comprend des moyens pour exploiter 20 en détection capacitive les six ou huit contacts métalliques 244 : sur présence d'un doigt nettement appuyé (ceci afin d'éviter l'effet que pourraient provoquer des portefeuilles ou porte-cartes en cuir), un signal positif vient positionner à 'vrai' le bit "transaction autorisée" (étape 310 sur la figure 3). Cette variante est particulièrement bien adaptée 25 à l'utilisation de la carte comme carte de paiement rapide ou comme "porte-monnaie électronique".

Dans la variante de la figure 8, le circuit détecteur 240 coopère avec des éléments à jauge de contrainte 246 permettant de détecter le fléchissement de la carte, comme illustré sur la figure. Sur détection de 30 carte fléchie (ce geste pouvant être très facile à acquérir par les usagers), un signal positif vient positionner à 'VRAI' le bit "transaction autorisée" (étape 310 de l'organigramme de la figure 3). En variante, la contrainte exercée peut être, au lieu d'une flexion, une pression exercée sur une zone particulière 247 de la carte repérée extérieurement.

35 Dans la variante de la figure 9, la carte 200 comporte une bande-

lette 248 en matériau ferromagnétique, du type de celles utilisées dans les magasins comme antivol pour disques ou livres. Cette bandelette comporte une combinaison d'alliages métalliques agencée de façon à entrer en résonance par détection d'hystéresis avec un champ 118 émis

5 par le terminal 100, comprenant lui-même des circuits électroniques oscillateurs et amplificateurs 120 pour la production de ce champ et des circuits de détection 122 du même type que ceux utilisés dans les systèmes antivol. Sur détection positive de la présence à faible distance d'une bandelette ferromagnétique 148, l'émetteur principal du terminal

10 est activé. Au contraire, en l'absence de bandelette — donc en l'absence de carte — les circuits électroniques de commande inhibent l'émetteur principal du terminal. Avantageusement, le champ nécessaire à la détection des bandelettes pourra être le même que le champ principal (référencé 102 sur la figure 1) lui-même nécessaire à la transaction.

15 Enfin, il est possible d'exploiter les caractéristiques offertes par l'antenne 202 de la carte, avec les composants qui forment le circuit accordé, pour détecter sa présence selon une méthode comparable à celle des anneaux antivol : une telle technique permet de n'émettre depuis le terminal qu'une puissance relativement faible pour pouvoir détecter en

20 retour, dans le champ électromagnétique, la présence du circuit accordé inclus dans la carte.

Dans la variante des figures 10 et 11, on incorpore dans l'épaisseur de la carte 200 des anneaux minces en matériau ferromagnétique (ferrite) d'épaisseur 0,1 mm environ. Sur la figure on a représenté cinq 25 de ces anneaux, mais ce nombre n'est pas limitatif, et l'on peut par exemple en prévoir un nombre de l'ordre de deux à vingt. Avant d'être noyés dans la matière plastique, certains de ces anneaux (262 sur la figure 11) sont sectionnés partiellement, d'autres (264 sur la figure 11) étant laissés intacts. On constitue ainsi une combinaison codée de tores 30 dont certains présentent un entrefer ouvert et d'autres un entrefer fermé vis-à-vis d'un champ magnétique émis par un circuit 124 du terminal 100 dans la région d'une fente d'insertion 126 recevant la carte et comportant cinq détecteurs spécialement agencés. Avantageusement, le champ nécessaire à la détection des tores pourra être le même que le 35 champ principal 102 lui-même à la nécessaire à la transaction.

Sur détection positive (présence du bon code formé par les cinq anneaux) l'émetteur principal du terminal est alors activé. Au contraire, en l'absence du code correct (donc en l'absence de carte), les circuits électroniques de commande inhibent l'émetteur principal du terminal.

5 Bien entendu, le terminal et l'ensemble du système sont agencés pour tenir compte des pertes occasionnées sous forme de courant de Foucault dans les anneaux métalliques 260.

Dans la forme de réalisation de la figure 12, le terminal 100 comporte un orifice à l'arrière duquel est monté un photodétecteur 128, lequel permet le déclenchement de l'émission du champ 102 via un circuit électronique 130 et un moyen interrupteur 132. Grâce à une bascule monostable 134, l'obscurité détectée par l'obturation du photodétecteur par application sur celui-ci de la carte 200 déclenche l'émetteur principal pour une durée la plus faible possible, par exemple 200 ms.

10 15 Les figures 13 et 14 illustrent une variante fonctionnant par télé-métrie, où une certaine distance entre la carte et le terminal est exigée pour l'entrée en fonctionnement de l'émetteur principal, afin que celui-ci ne soit pas intempestivement déclenché par des cartes qui, se situant par exemple à plus de 50 cm, ne seraient de toutes façons pas en état de 20 communiquer avec le terminal. Il est possible d'utiliser une méthode par phototélémétrie afin de n'exploiter que les cartes se trouvant le plus précisément possible dans les conditions utiles, par exemple une vingtaine de centimètres. A cet effet, on mesure le temps de propagation du rayon lumineux entre son point de départ (diode électroluminescente 136 du terminal) et son point d'arrivée (photodiode 138 du 25 terminal) :

— exploitation d'une horloge rapide (par exemple 100 MHz) 140 sur les entrées 142 et 144 (correspondant respectivement aux signaux illustrés sur la figure 14) d'une porte OU EXCLUSIF 146, dont le signal de sortie 148 est également illustré figure 14 ;
30 — retard sur l'entrée 144 provoqué par le temps de propagation aller-retour du rayon lumineux (pour une carte située à 10 cm du terminal : 0,6 ns) ; à une distance très courte, par exemple 1 mm, la sortie 148 de la porte 146 offre un signal quasi-plat, puisque les impulsions logiquement créées sont d'une durée très inférieure au 35

5 temps de réaction de la circuiterie, de l'ordre de 6 ps ;

— au contraire, une durée d'impulsion (signal 148) de l'ordre de 0,6 ns (pour un cycle total de 10 ns) constitue une grandeur mesurable avec des composants de caractéristiques appropriés, notamment par intégration : circuit RC 150, 152 délivrant une tension V 154 inversement proportionnelle à la distance entre la carte et le terminal (on devra bien entendu tenir compte des constantes de temps du circuit et des composants qui influent sur les temps de montée et de descente sur les signaux) ;

10 — en variante, une bascule monostable 156 peut être déclenchée par une impulsion de 0,6 ns créant elle-même sur la sortie Q (dans le cas où la distance entre carte et terminal est supérieure à 20 cm) une impulsion de durée par exemple égale à 150 ms, soit nécessaire au déroulement automatique de la transaction complète.

15 Dans l'exemple des figures 15 à 17, on prévoit sur le terminal un ensemble comportant un ou plusieurs émetteurs de lumière 158 coopérant avec une pluralité de photorécepteurs 160 tels que photodiodes ou autres, assemblés par exemple sur un module de 1 cm^2 . Avantageusement, les photodiodes sont équipés d'un système optique tel qu'une lentille permettant de capter sous plusieurs angles le rayon réfléchi par la carte, de façon à ne pas exiger une présentation de la carte dans une position par trop prédéterminée, qui serait contraignante pour l'usager.

20 Avantageusement, un système optique particulier pourrait comprendre, comme illustré figure 16, une pluralité de miroirs semiréfléchissants 162 inclinés à 45° dans l'axe des diodes électroluminescentes 164, les photorécepteurs 166 étant disposés perpendiculairement à l'axe des émetteurs lumineux.

25 La configuration de la figure 16 peut, en variante, être remplacée par celle de la figure 17, l'émetteur-récepteur comportant une pluralité de diodes émettrices 168 et une photodiode 170 légèrement enfoncée par rapport au plan des diodes émettrices 168 (ou l'inverse) de façon à ne pas être éblouie par la lumière 172 produite par ces dernières, mais recevant uniquement l'énergie lumineuse 174 renvoyée par le matériau réfléchissant 266 de la carte 200.

30 Dans la variante des figures 18 et 19, on prévoit dans la carte une

puce 268 comprenant :

- des plots 270 destinés à la connexion de la bobine 202, ainsi qu'éventuellement des plots 272 destinés à la connexion aux divers contacts (dans le cas d'une carte mixte contact/sans contact),
- 5 — un ou plusieurs éléments photodétecteurs 274 tels que photodiode ou phototransistor, structure photovoltaïque, etc,
- une couche de matériau opaque 276, où un orifice 278 (figure 19) permet le passage de la lumière vers le photodétecteur 274, tandis que les autres organes de la puce, et notamment les mémoires programmables, effaçables ou réinscriptibles telles qu'EPROMs ou EEPROMs qui peuvent être sensibles au rayonnement lumineux, sont protégés de la lumière.

Dans une variante de réalisation, une fenêtre protectrice peut être agencée à l'extérieur du semiconducteur, de façon par exemple à ne pas grever son coup. Ainsi, l'enrobage 280 de la puce (en PVC, ABS, etc.) pourra comporter un tel orifice 278, à condition que celui-ci soit usiné et positionné avec précision ; les dimensions de l'orifice sont de l'ordre de 0,1 ou 0,01 mm selon la finesse de gravure de l'ensemble et des caractéristiques optiques du matériau et son usinage.

20 Quant à la carte 200, qui est illustrée figure 20, il est prévu sur le corps de celle-ci, de préférence le plus près possible de la puce, une surface photoréfléchissante 214 telle que cataphote, catadioptrre ou bande adhésive rétroréfléchissante. La fonction de réflexion de lumière peut également être obtenue par un usinage ou traitement particulier de l'enrobage, incluant par exemple des particules d'aluminium.

Sur la figure 21, on a illustré le fonctionnement du système selon un mécanisme de "reconnaissance mutuelle" exploitant les caractéristiques de reconnaissance propres à la combinaison des effets électromagnétiques et photoélectriques, telles que :

- 30 — le terminal ne soit autorisé à fonctionner (à émettre) que sur reconnaissance de la présence d'une carte, et
- la carte ne soit autorisée à fonctionner (à écrire en mémoire) que sur reconnaissance de la présence d'un terminal.

35 Ce mécanisme se décompose en trois étapes successives, qui sont de nature soit optique soit électromagnétique :

- optiquement, un terminal 100 reconnaît une carte 200 par émission d'un rayon lumineux 176, réflexion en 282 par le photoréflecteur 214 de la carte 200, puis réception par le photodétecteur 106 du terminal,

5 — électromagnétiquement, la carte et le terminal entrent en dialogue, à l'initiative du terminal (émetteurs/récepteurs de part et d'autre),

- optiquement, la carte attend du terminal un signal d'autorisation 178, exploité par le semiconducteur 210, qui valide le dialogue et permet l'écriture dans la mémoire.

10 Plus précisément, dans ce cas où l'on combine un détecteur optique d'approche (sur le terminal) à un détecteur d'action volontaire du porteur (sur la carte), les étapes successives de communication sont les suivantes :

- 1) le terminal émet en permanence un rayon lumineux (donc sans risque biologique), éventuellement modulé,

15 2) à l'approche d'une carte, cette émission lumineuse est réfléchie passivement vers le terminal,

20 3) le terminal capte le rayon réfléchi, traite et décode le signal récupéré afin d'éliminer les effets de la lumière ambiante, et le signal résultant donne une indication de l'approche ou de la présence d'un utilisateur,

25 4) le terminal sort de son état quiescent et émet le champ électromagnétique principal,

30 5) la carte reçoit le champ électromagnétique, en extrait l'énergie nécessaire à son alimentation interne, démodule le signal et active le microprocesseur ainsi que la photodiode de détection intégrée,

35 6) le microprocesseur de la carte dialogue sans contact avec le terminal puis, avant de débiter le montant prévu, interroge la photodiode intégrée à la carte, laquelle génère un signal logique après traitement et décodage du courant généré par le rayon ; sur détection positive, le microprocesseur de la carte valide l'autorisation de paiement, procède à l'inscription dans la mémoire de la carte et poursuit ou achève la transaction.

On va maintenant décrire en référence aux figures 22 à 28 un certain nombre de formes de réalisation particulières adaptées à une carte incorporant des moyens photodétecteurs.

On a en effet indiqué plus haut que, pour éviter les risques de "vol à la tire électronique", on fait en sorte qu'une partie au moins de la communication entre la carte et le terminal soit rendue conditionnelle sur une action volontaire de la part de l'utilisateur, cette action volontaire pouvant avantageusement être captée par la détection d'une lumière (la fonction de communication étant rendue conditionnelle sur la présence ou l'absence de cette détection de la lumière).

On a également décrit une carte comportant à cet effet un détecteur de lumière ambiante avec un élément photosensible (référencé 274 sur les figures) tel qu'une photodiode, un phototransistor ou un élément photovoltaïque par exemple, l'action volontaire consistant à sortir la carte de manière à activer ce détecteur de lumière ambiante.

Sur la figure 22, l'élément photosensible 274 produit, après amplification et seuillage, un signal logique LUX qui permettra d'autoriser (ou non) le fonctionnement de la carte du fait de l'éclairement de celle-ci, éclairement qui, comme on l'a indiqué plus haut, peut être le fait de la seule lumière ambiante.

En d'autres termes, pour autoriser la transaction, il suffit à l'utilisateur de sortir la carte de son portefeuille et de l'exposer à la lumière ambiante, ce simple geste autorisant le déroulement subséquent de la transaction, par exemple l'écriture d'un crédit ou d'un débit en mémoire. On soulignera que, dans cette mise en oeuvre à détection de la lumière ambiante par la carte, il est possible d'utiliser des terminaux classiques, non pourvus de moyens optoélectroniques ; la détection de la lumière ambiante par la carte vient simplement ajouter un niveau de sécurité supplémentaire, côté carte, pour autoriser la poursuite de la transaction par cette dernière avec le terminal, le reste de la transaction se déroulant de manière en elle-même classique.

Un bistable 300 commande une entrée spécifique WRITE_INHIBIT du microcircuit 268 (cf. figure 18), qui interdira l'écriture en mémoire. L'état du bistable 300 est contrôlé, d'une part, par le signal LUX et, d'autre part, par divers signaux appliqués par une logique de coman-

de 302, qui est en fait un sous-ensemble du microcircuit 268).

La bascule 300 est remise à zéro par l'impulsion initiale positive de remise à zéro générale de la puce, peu après la mise sous tension de cette dernière, elle-même consécutive à la réception du champ (et donc 5 de l'énergie) électromagnétique émis par le terminal.

Dans l'obscurité, le photodétecteur 274 engendre sur l'entrée 304 de la porte 306 un signal LUX à l'état bas. Dès la retombée de l'impulsion initiale de remise à zéro, la bascule 300 est ainsi positionnée à '1' sur sa sortie 308 (WRITE_INHIBIT), interdisant l'écriture.

10 En revanche, si la carte est, par exemple, sortie de son étui ou d'un portefeuille et présentée dans une ambiance lumineuse, la commande WRITE_INHIBIT devient inactive, autorisant donc l'écriture, du moins pour la durée de la transaction.

15 Ainsi, l'opération de "vol à la tire électronique" consistant à approcher de la carte-cible un faux terminal portatif munis d'une antenne adéquate afin de mettre en service indûment la carte dans le but d'y enregistrer une opération de débit est impossible tant que la carte réside dans l'obscurité d'une poche, d'un portefeuille, d'un sac à main, etc. L'utilisateur est donc garanti contre ce risque de fraude particulièrement 20 pernicieux.

25 Dans une variante de mise en oeuvre, on peut prévoir que cette sécurité soit rendue optionnelle, au choix de l'industriel fabriquant la carte protégée. En effet, pour les besoins de tel ou tel client, il peut être souhaitable que cette sécurité puisse être à volonté systématiquement activée ou désactivée au stade de la fabrication/personnalisation des cartes.

30 A cette fin, on affecte un emplacement particulier de la mémoire à un indicateur déterminant cette consigne. Cet indicateur, situé à une adresse ADDRESS_PROTECT_WRITE (AD_PROT_W), est lu sur la sortie de données DATA_OUT (DOUT) de la mémoire. Selon que ce bit indicateur est enregistré en usine à '0' ou à '1', la lecture de la mémoire provoquera ou non, lors d'une transaction, le basculement du bistable 300, inhibant ainsi, ou non, la sécurité apportée par le détecteur optique décrit précédemment.

35 Un autre risque lié à l'utilisation des cartes à puce sans contact est

celui de l'indiscrétion ou de l'espionnage, par exemple du fait d'une volonté malveillante de prendre connaissance, à l'insu de son porteur, du contenu de sa carte (ce type de risque n'existant pas, bien entendu, avec les cartes à contacts galvaniques).

5 C'est pourquoi il peut être souhaitable de rendre également conditionnelle la commande de lecture, plutôt que la seule opération d'écriture. Pour ce faire, selon l'invention, on décode le contenu d'une adresse spécifique ADDRESS_PROTECT_READ (AD_PROT_R), qui pourra par exemple être adjacente à l'adresse ADDRESS_PROTECT_WRITE. La carte est alors pourvue d'un bistable 310, semblable au bistable 300 et susceptible de produire sur sa sortie 312 un signal READ_INHIBIT conditionnant le fonctionnement en lecture de la mémoire du microcircuit de la carte, de la même manière que le signal WRITE_INHIBIT en conditionnait l'écriture.

10 15 On peut également prévoir une porte OU (non représentée) activée par les deux signaux READ_INHIBIT et WRITE_INHIBIT pour générer un signal d'inhibition générale, en lecture et écriture.

20 Ainsi, sans élargir sa gamme de produits, le fabricant pourra indifféremment proposer soit une carte à puce sans contact traditionnelle, soit la même carte sécurisée en outre contre "l'accès nocturne", c'est-à-dire contre les tentatives de lecture et/ou écriture dans l'obscurité. Ceci, pour le faible coût de quelques composants (moins de dix portes), ainsi qu'un traitement spécifique de la surface du plastique et/ou du circuit intégré (comme décrit plus haut en référence aux figures 18 et 19, et plus bas en référence aux figures 26 à 29).

25 La séquence de mise en oeuvre peut s'exprimer par la succession d'étapes de processus suivante.

Début

30 *Remise à zéro générale*
AD = 0
WRITE_INHIBIT = 0
READ_INHIBIT = 0
...
35 Lecture DATA_OUT

```
IGNORE_WRITE = DATA_OUT (AD)
IGNORE_READ = DATA_OUT (AD +1)
...
WRITE_INHIBIT = (IGNORE_WRITE) NOR (LUX)
READ_INHIBIT = (IGNORE_READ) NOR (LUX)
```

5 READ_INHIBIT = (IGNORE_READ) NOR (LUX)

Suite de la transaction

• • •

Fin

10

Au moment de l'initialisation générale de la puce, les indicateurs correspondant aux deux inhibitions possibles sont mis à zéro (WRITE_INHIBIT = 0 et READ_INHIBIT = 0) en même temps que le compteur d'adresse (AD = 0). Deux indicateurs IGNORE_WRITE et IGNORE_READ reflètent quant à eux le contenu des adresses correspondantes de la mémoire, respectivement AD = 0 et AD = 1.

La lecture des deux positions initiales de la mémoire, données par l'ordre "Lecture DATA_OUT", fournit par exécution d'une fonction NOR avec l'état LUX du photodétecteur le statut des deux commandes d'inhibition WRITE_INHIBIT et READ_INHIBIT.

La figure 23 illustre une variante de réalisation permettant une invalidation conditionnelle du circuit inhibiteur, c'est-à-dire permettant dans certains cas particuliers déterminés un "fonctionnement nocturne" du circuit intégré, c'est-à-dire autorisant le fonctionnement malgré l'absence de lumière ambiante.

Ainsi, dans le cas d'une carte d'identification ou de péage pour l'accès à une zone contrôlée, il est souhaitable que les porteurs de la carte soient identifiés et/ou débités d'un certain montant lors de leur entrée dans la zone, ou en début de journée. Cette transaction est opérée de façon conventionnelle avec présentation de la carte (donc avec exposition à la lumière ambiante) devant un lecteur destiné à cette fonction.

Pour autant, il serait contraignant de devoir contraindre les porteurs à sortir la carte de leur poche ou de leur portefeuille lors de chacun de leurs passages ultérieurs, ou à la sortie de la zone, ou pendant un certain temps de présence autorisé à l'intérieur du site, etc.

Pour cela, selon une autre caractéristique du système de l'invention, on prévoit une invalidation conditionnelle du dispositif de protection décrit précédemment.

Une adresse spécifique AD_INV_NOC contient un indicateur spécifique affecté à cette fonction qui, en combinaison avec un contenu pré-déterminé de la mémoire, par exemple '1', positionnera une bascule 314 via une porte 316. Le signal INV_NOC (Invalidation de la protection Nocturne) ainsi produit en sortie du bistable 314 est dirigé sur une entrée particulière supplémentaire 318 du bistable 300 de façon à positionner à '0' le signal WRITE_INHIBIT, et ceci indépendamment de l'état du signal LUX représentatif de l'absence ou de la présence de lumière sur l'élément photosensible 274.

Le mode opératoire sera le suivant : lors de l'entrée sur le site, le porteur extrait la carte de son portefeuille, de sa poche, de son sac à main, ... de façon à l'exposer à la lumière ambiante. Le terminal commence par effectuer sur la mémoire de la carte les opérations de lecture, et éventuellement d'écriture, nécessaires au contrôle de l'accès au site. Après quoi, le terminal écrit à l'adresse AD_INV_NOC la valeur convenue, de façon à pré-déterminer à 'VRAI', ultérieurement, le paramètre INV_NOC.

Ainsi, lors de son prochain passage devant un terminal, la carte n'aura pas besoin d'être éclairée et pourra donc rester en poche, pour autant que la distance d'exploitation (distance entre carte et terminal) le permette. Les opérations d'écriture et/ou de lecture interviendront alors inconditionnellement : en effet, dès sa mise sous tension, et dès réception du signal d'horloge, le microcircuit aura adressé la position AD_INV_NOC et lu son contenu (INV_NOC = '1'). Le terminal pourra exécuter toutes opérations nécessaires au contrôle de la situation, en particulier vis-à-vis de la carte, dont il pourra utilement remettre à zéro (ou, plus généralement, mettre à jour) le contenu de l'adresse AD_INV_NOC.

La figure 24 illustre un mode de réalisation particulier permettant une acquisition conditionnelle des consignes. Dans ce mode de réalisation, l'état de trois variables est positionné dès la mise sous tension (RESET) du microcircuit : présence de lumière (LUX), consigne IGNORE_WRITE et consigne IGNORE_READ. Les deux premières données sont

prises en compte lors de l'adressage de la mémoire à l'adresse zéro (AD = 0), et la dernière lors du passage à l'adresse suivante (AD = 1).

5 Les portes ET 318 et 320 échantillonnent la sortie DOUT(0) correspondant au contenu de la mémoire à l'adresse zéro (AD = 0). Les bistables 322 et 324 conservent cette consigne le temps d'une transaction. La porte ET 326 échantillonne le contenu DOUT (1) de la mémoire lors du passage à l'adresse AD = 1, et le bistable 328 qui conserve cette consigne le temps de la transaction. Enfin, les portes NOR 330 et 332 fournissent les signaux d'inhibition WRITE_INHIBIT et READ_INHIBIT.

10 Les figures 25 à 29 illustrent des aspects technologiques particuliers avantageux pour la réalisation d'une carte incorporant des moyens photodétecteurs du type illustré sur les figures 18 et 19.

15 La figure 25 illustre ainsi un circuit de compensation automatique de l'alimentation du microcircuit 268 en fonction du niveau d'éclairage éventuel, pour éviter des risques de dysfonctionnements du microcircuit par éclairage parasite des composants. Ce phénomène parasite pourrait d'ailleurs être exploité de façon malveillante par un fraudeur qui souhaiterait passer outre les sécurités incorporées à la carte en créant délibérément des dysfonctionnements de manière à provoquer l'ouverture intempestive de portes, le positionnement de bascules dans un état différent de celui prévu par les équations logiques, etc., tous phénomènes susceptibles de se produire lorsque la carte est amenée à fonctionner hors des conditions nominales prévues.

20 Avec le circuit de compensation de la figure 25, le signal issu du photodétecteur 274, convenablement traité par l'amplificateur spécifique 334, assure le contrôle de l'alimentation générale du microcircuit 268 (ou, tout au moins, de la fraction la plus vulnérable de ses organes) via un circuit de régulation programmable 336 placé sur la ligne d'alimentation V_{CC} . Indépendamment de ce contrôle exercé sur l'alimentation, une action correctrice peut être exercée sur une entrée spécifique de polarisation 338 du microcircuit, susceptible d'intervenir sur le gain ou le seuil des étages sensibles.

25 Une autre protection qu'il est important de mettre en oeuvre consiste à guider la lumière entrante vers le point cible (zone photodétectrice sensible du microcircuit) en évitant l'éclairage des composants

autres.

Ainsi, sur les figures 26 à 28, la zone photosensible 340 s'étend le long de l'un des côtés de la puce 268, et la lumière arrive via un orifice 342 ménagé au travers du substrat 344, la lumière pénétrant donc, 5 comme illustré en 346 sur la figure 27, du côté du substrat 344 opposé à celui où se trouve la puce du microcircuit 268.

Pour guider la lumière vers la seule zone photosensible 340, on exploite le caractère réfléchissant des fils métalliques destinés à la prise de connexion ("bonding") de la puce 268. A cet effet, un des fils 348 est 10 formé avant soudure avec une section U (voir notamment figure 28) lui donnant une forme de gouttière inversée, la partie creuse 350 étant tournée vers la surface photosensible 340 de la puce de microcircuit 268. Une fois le fil soudé sur le plot de connexion 350, sa cambrure (visible notamment figure 27) lui permet de se comporter comme un conduit spécifique de lumière, celle-ci arrivant via l'orifice 342 et étant guidée par le fil vers la seule zone photosensible 340.

Dans une autre variante de réalisation, illustrée figure 29, dans le but d'éviter qu'un quelconque rayon lumineux n'atteigne la surface du microcircuit portant les différents composants logiques (composants situés sur le côté référencé 352 sur la figure 29), on dispose l'organe photodétecteur 274, ici sous forme de composant rapporté, à côté de la puce de microcircuit 268, mais verticalement retourné, c'est-à-dire avec sa surface sensible tournée dans le sens opposé à celui de la surface 352. À cette fin, on exploite la possibilité offerte lors du montage du microcircuit sur un "micromodule" de carte à puce constitué d'un circuit imprimé en forme de substrat 344 très mince. Des pistes adéquates telles que 354 sont prévues sur le substrat 344 du micromodule de façon à pouvoir connecter par soudure les plots 356 du composant photosensible 274 et les plots 358 du microcircuit retourné 268.

REVENDICATIONS

1. Un système pour la communication sans contact entre un terminal (100) et un objet portatif tel qu'une carte (200), le terminal et la carte comportant chacun des moyens émetteurs-récepteurs de champ électromagnétique et la carte comportant une puce (210) avec des circuits de traitement et une mémoire (228) inscriptible sur commande du terminal,
5 caractérisé en ce que la carte comporte des moyens de validation, conditionnant au moins une étape du déroulement de la communication à une action prédéterminée extérieure de confirmation exercée avec cette carte par le porteur de la carte, ces moyens de validation comportant, dans la carte, des moyens récepteurs de lumière coopérant avec les circuits électroniques de traitement numérique et avec la mémoire.
- 10 15 2. Le système de la revendication 1, dans lequel l'action prédéterminée de confirmation est l'exposition de la carte à l'éclairement ambiant.
- 20 25 3. Le système de l'une des revendications 1 ou 2, dans lequel la mémoire contient une donnée formant indicateur d'activation ou d'inhibition des moyens de validation indiquant si, respectivement, ladite étape du déroulement de la communication doit ou non être conditionnée à ladite action prédéterminée extérieure de confirmation.
- 30 4. Le système de la revendication 3, dans lequel l'indicateur d'activation ou d'inhibition est une donnée statique prédéterminée.
5. Le système de la revendication 4, dans lequel la donnée statique est irréversiblement prédéterminée.
- 35 6. Le système de la revendication 3, dans lequel l'indicateur d'activation ou d'inhibition est une donnée modifiable dynamiquement par une borne lors du déroulement d'une communication.

7. Le système de l'une des revendications 1 à 6, dans lequel l'étape conditionnelle du déroulement de la communication est l'activation de l'écriture de la mémoire de la carte.

5 8. Le système de l'une des revendications 1 à 7, dans lequel l'étape conditionnelle du déroulement de la communication est l'activation de la lecture de la mémoire de la carte.

10

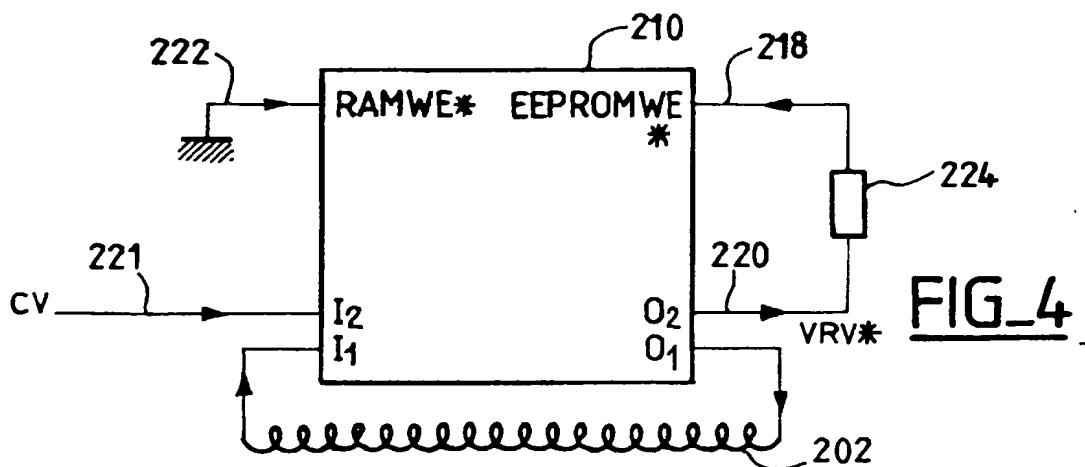
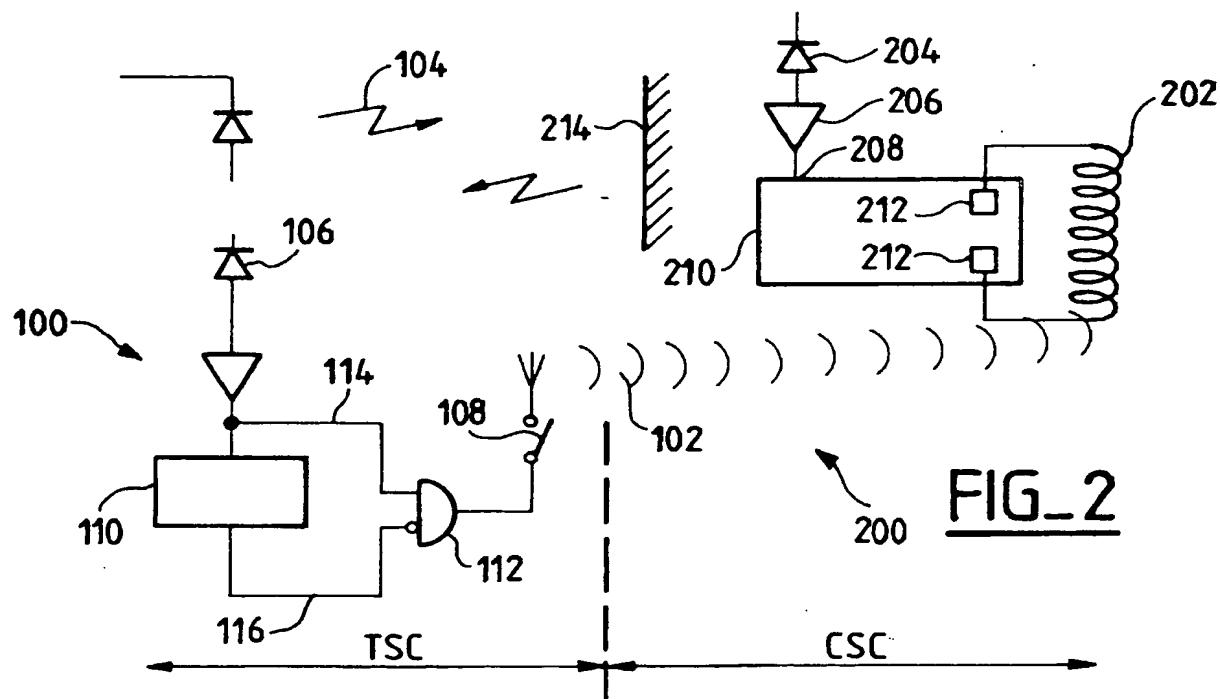
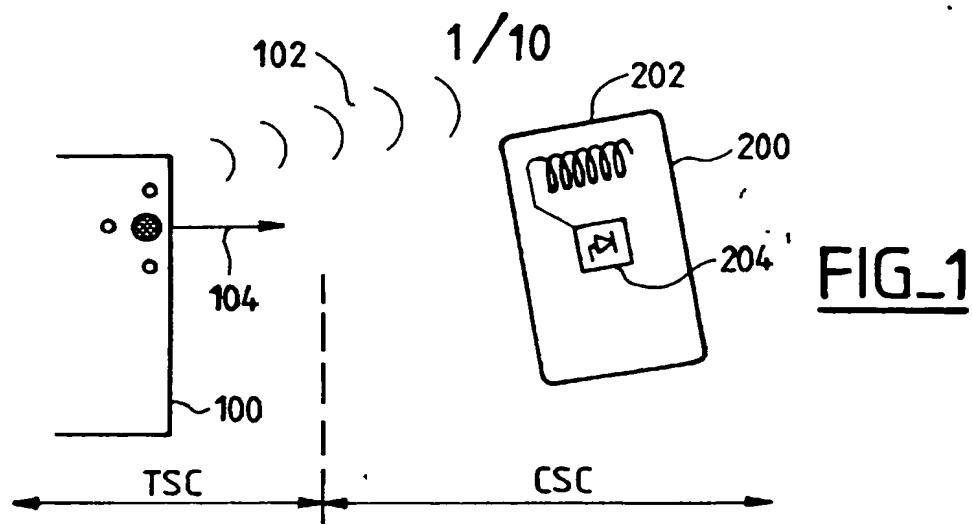
15

20

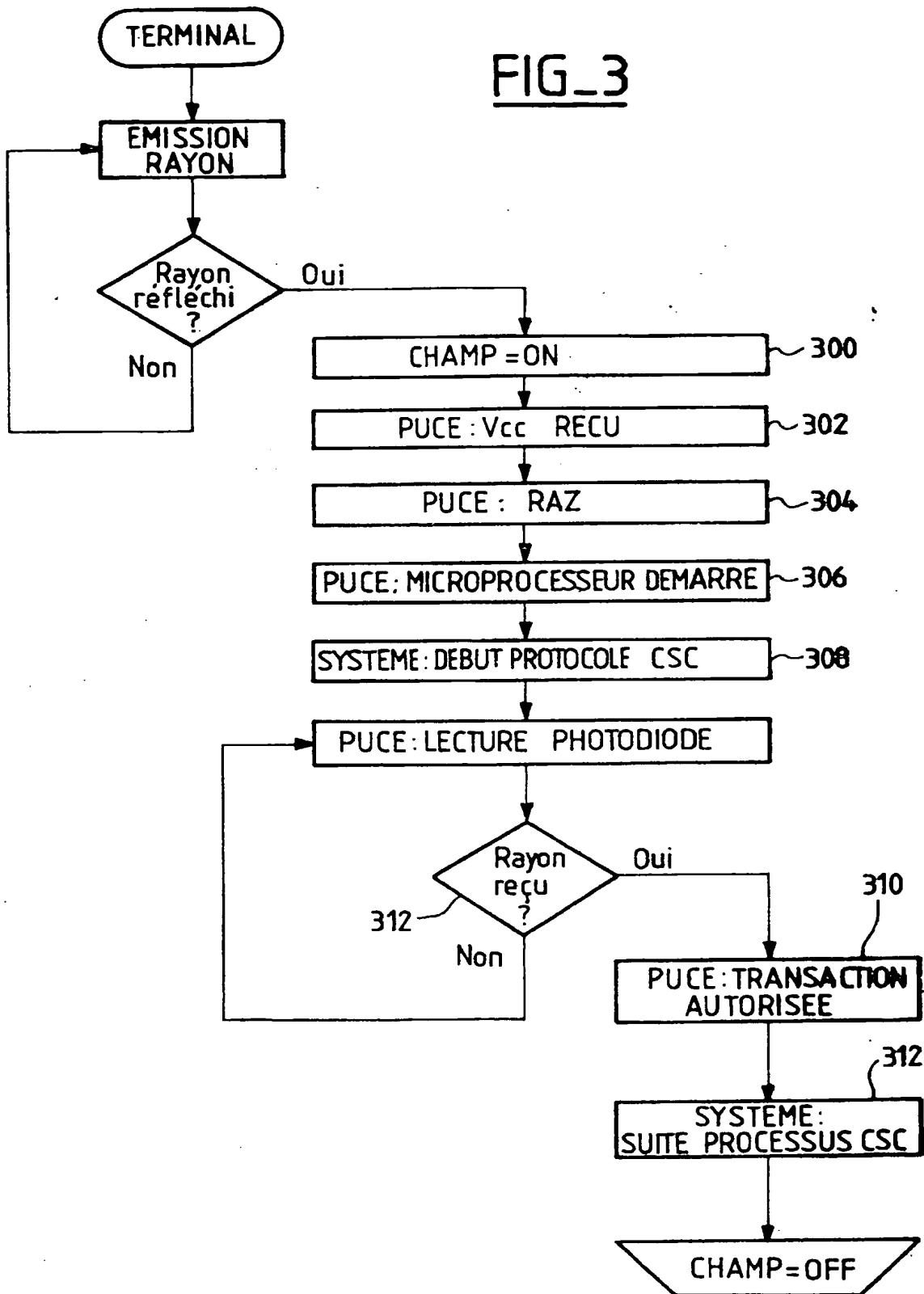
25

30

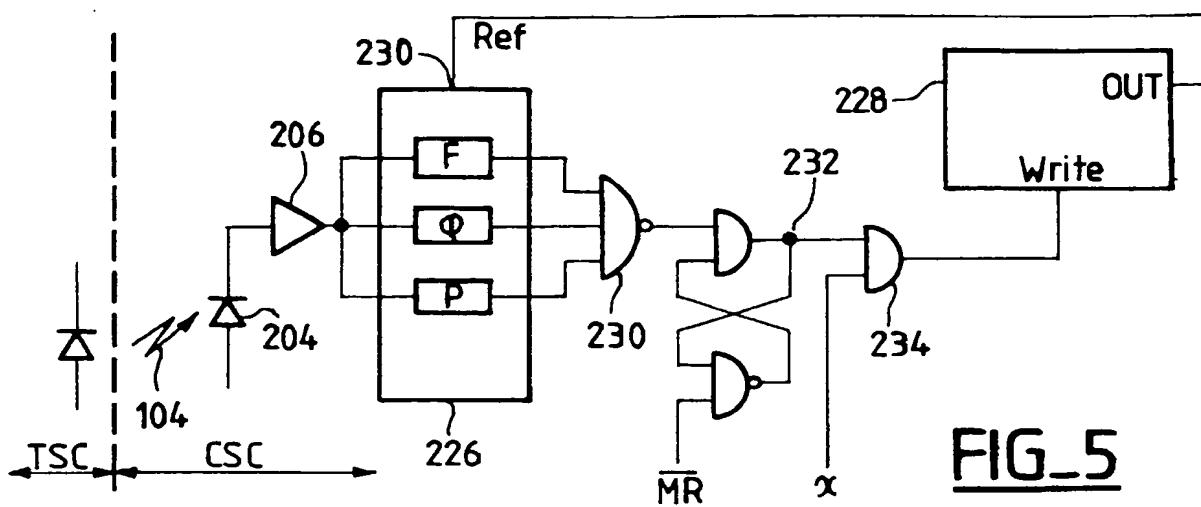
35



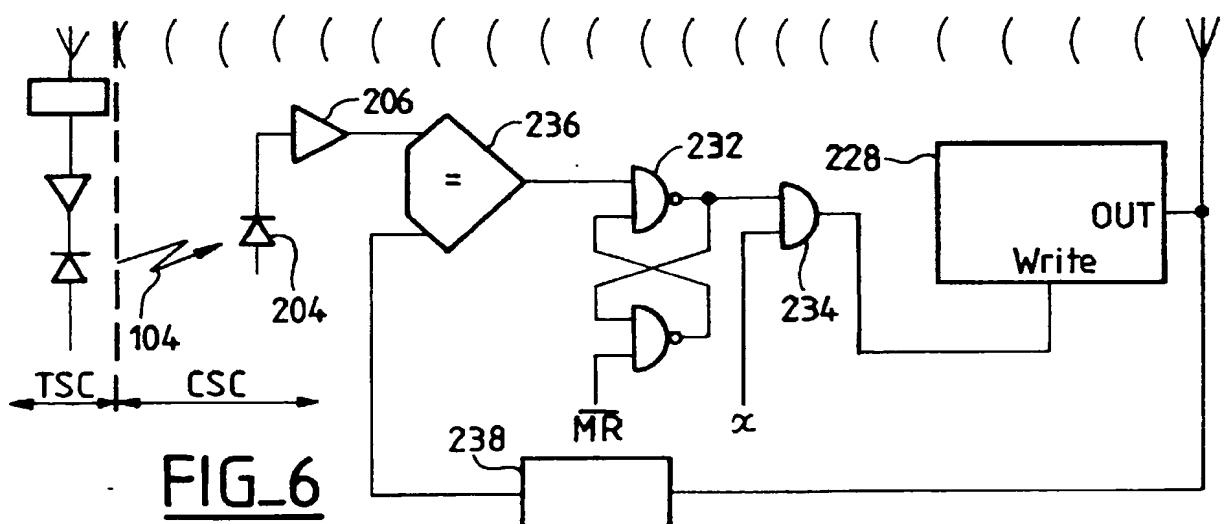
2 / 10



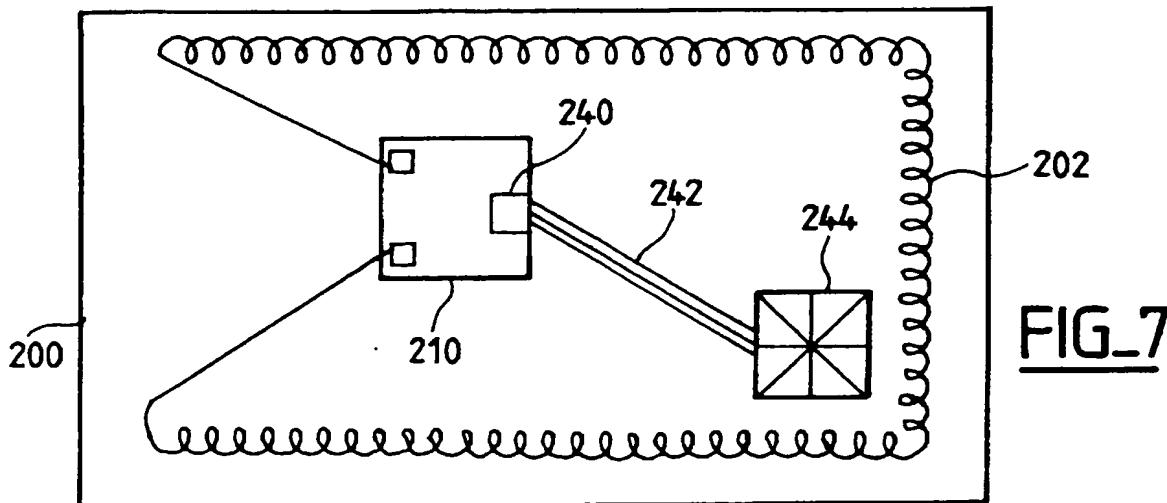
3/10



FIG_5

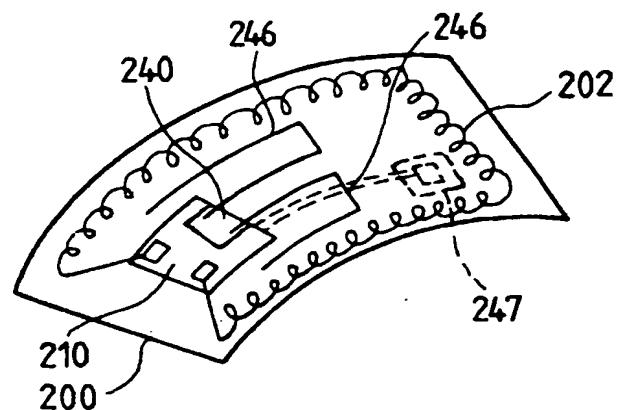


FIG_6

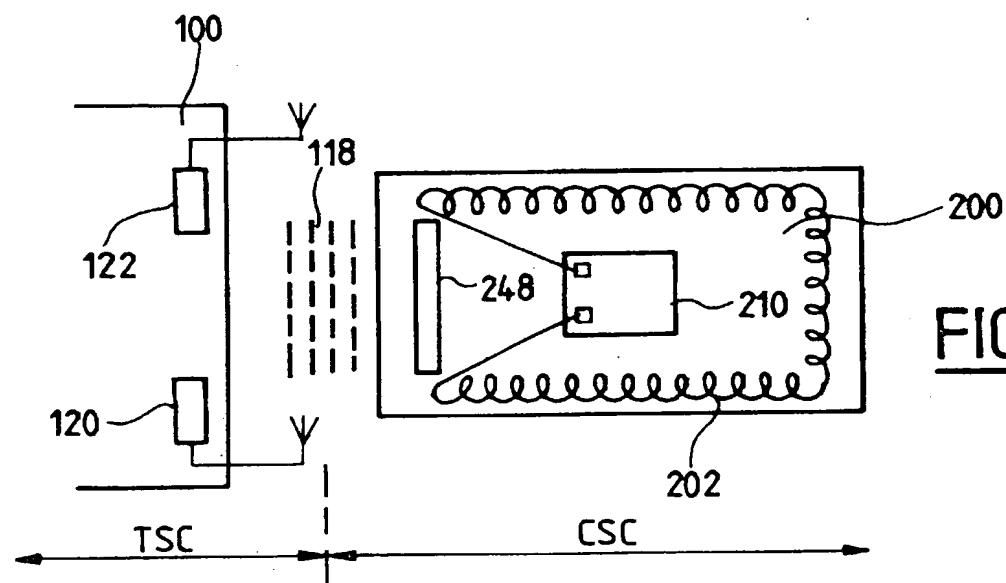


FIG_7

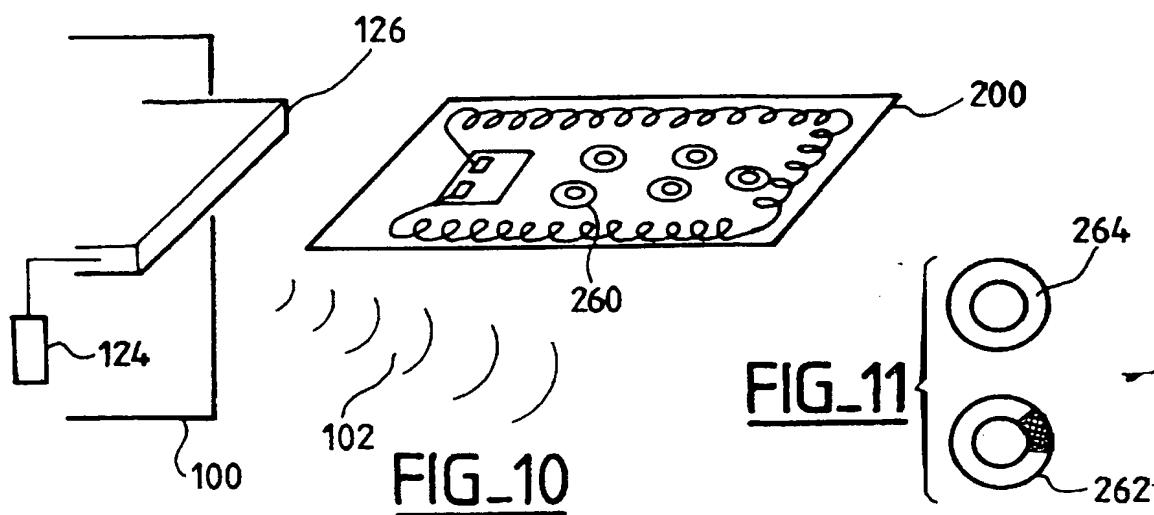
4/10



FIG_8



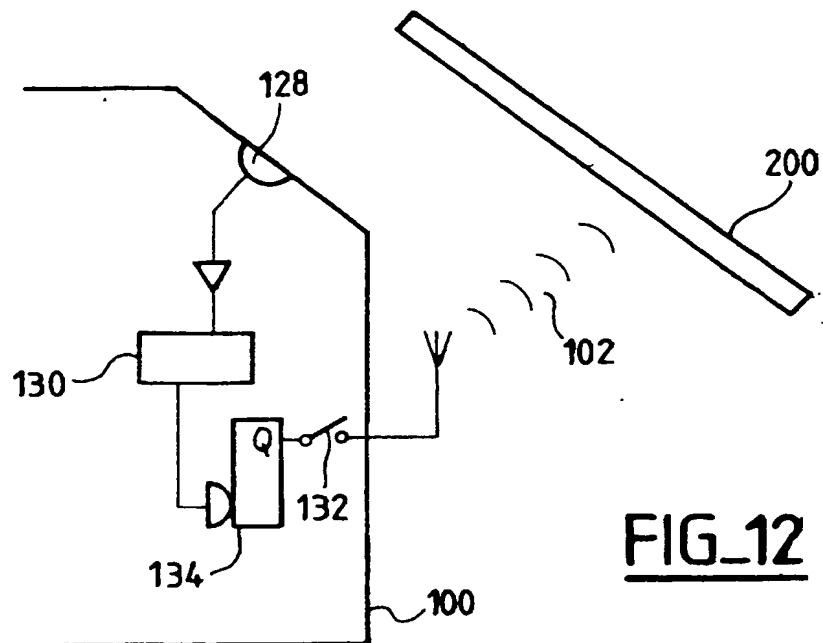
FIG_9



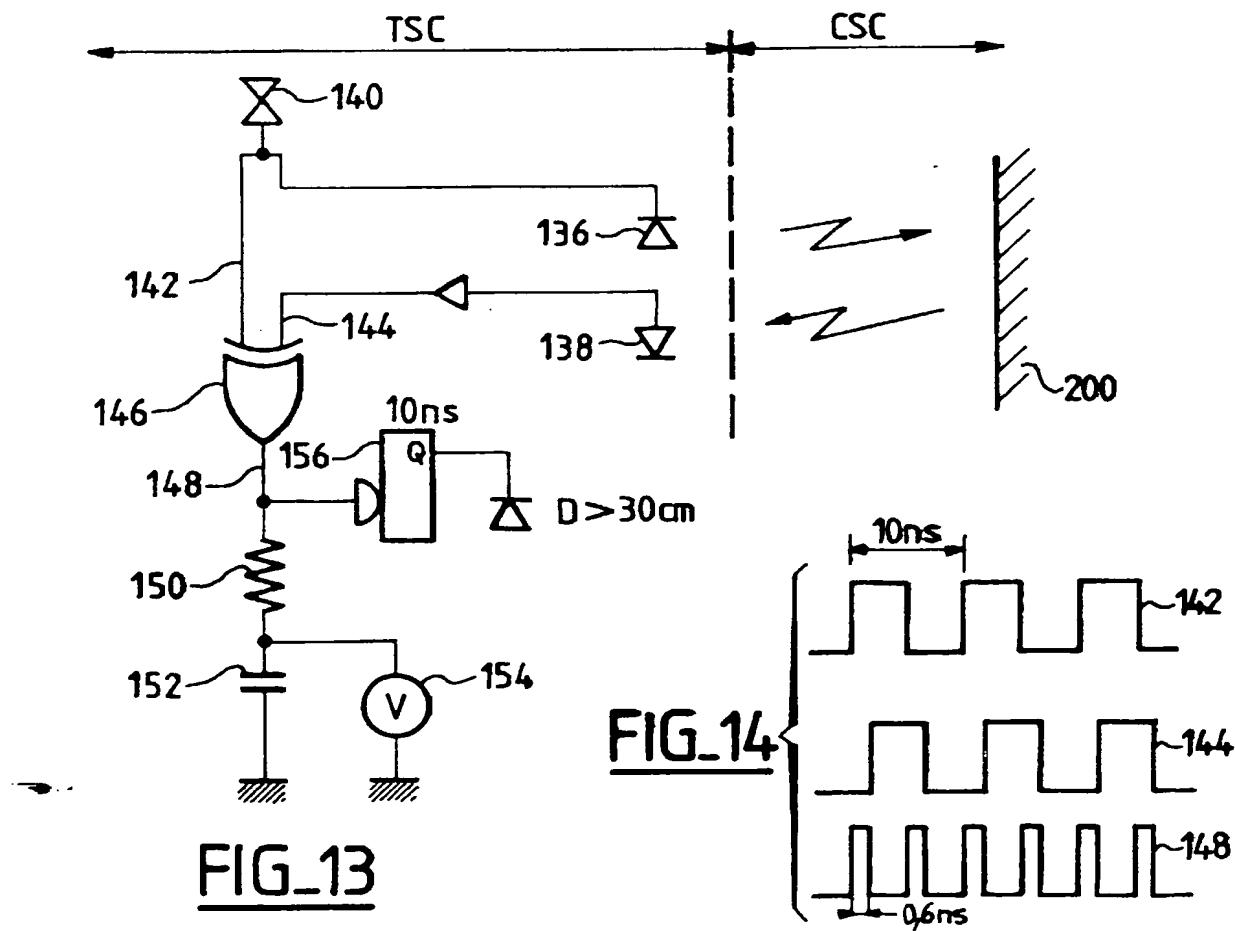
FIG_10

FIG_11

5/10



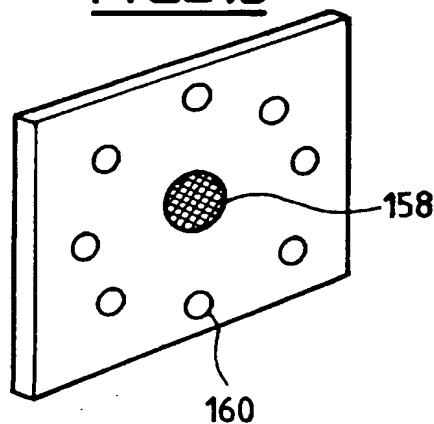
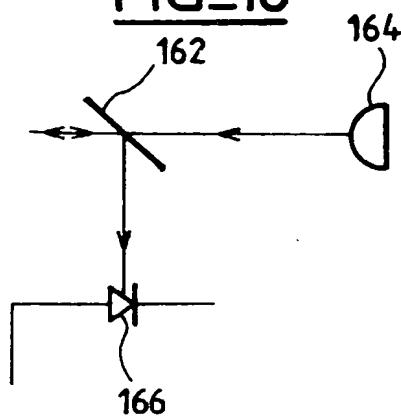
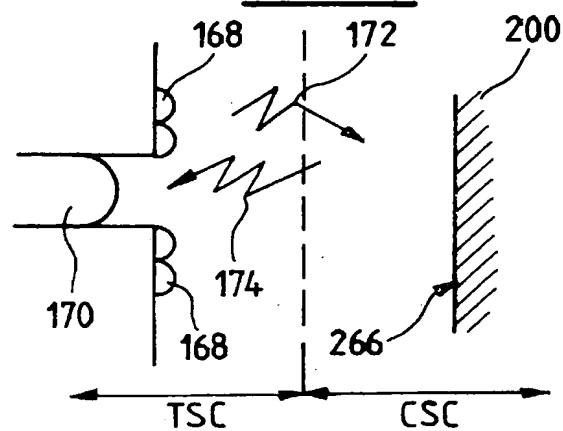
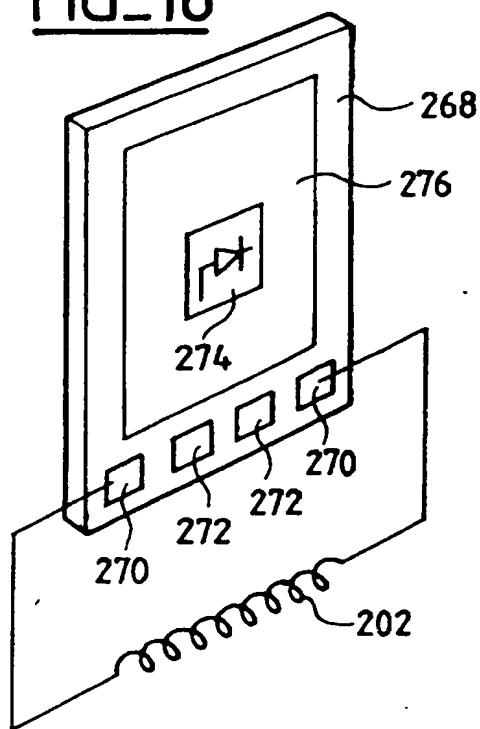
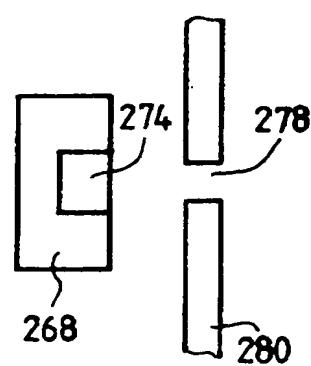
FIG_12



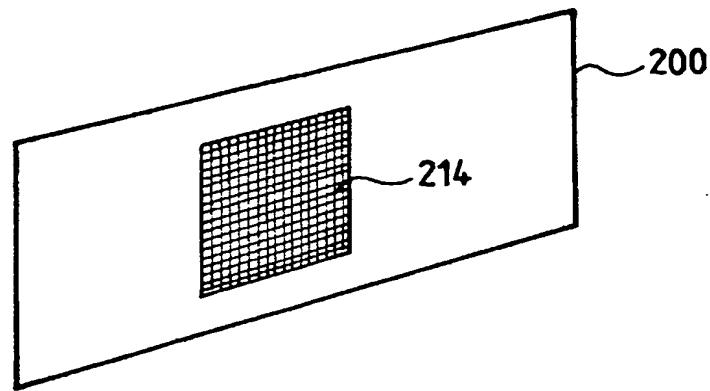
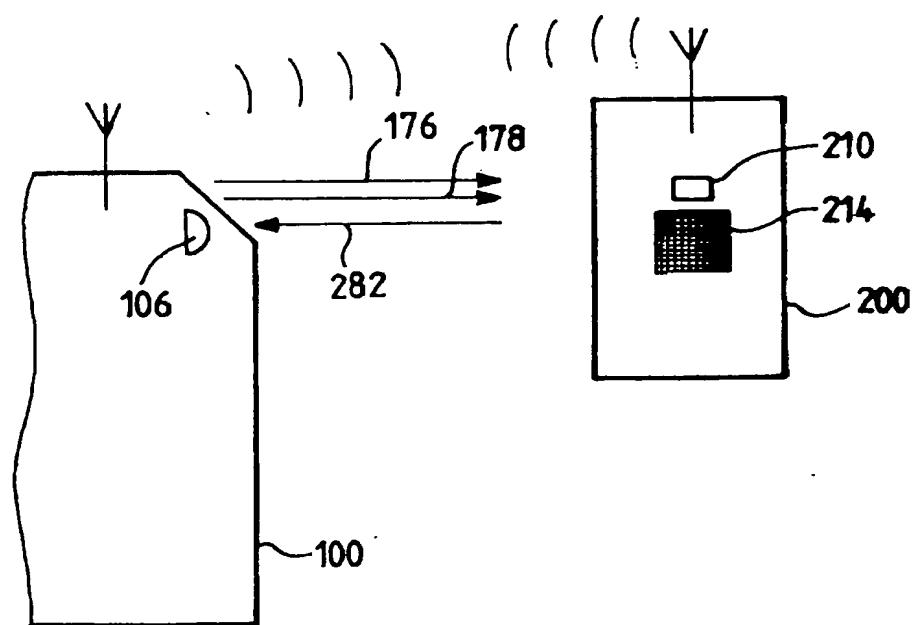
FIG_13

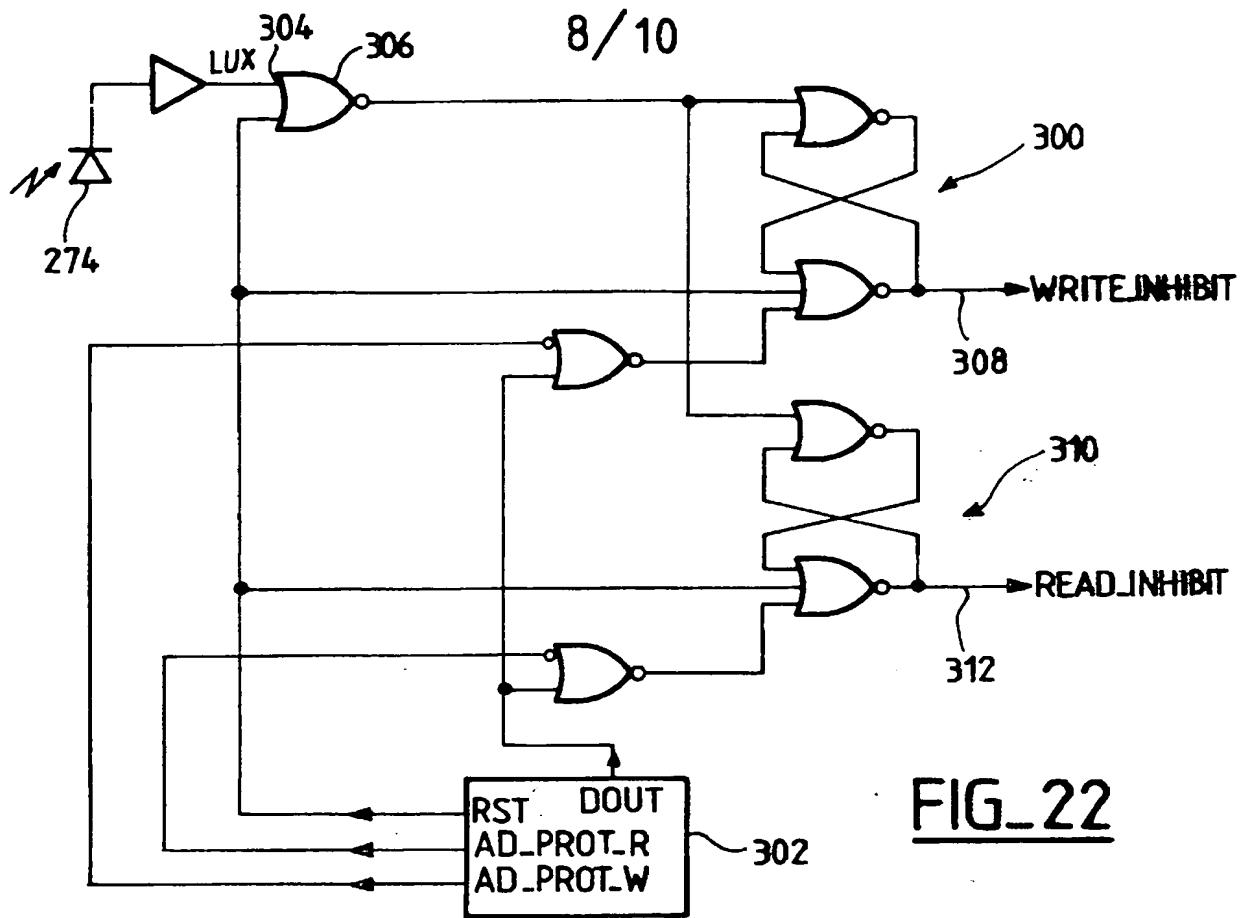
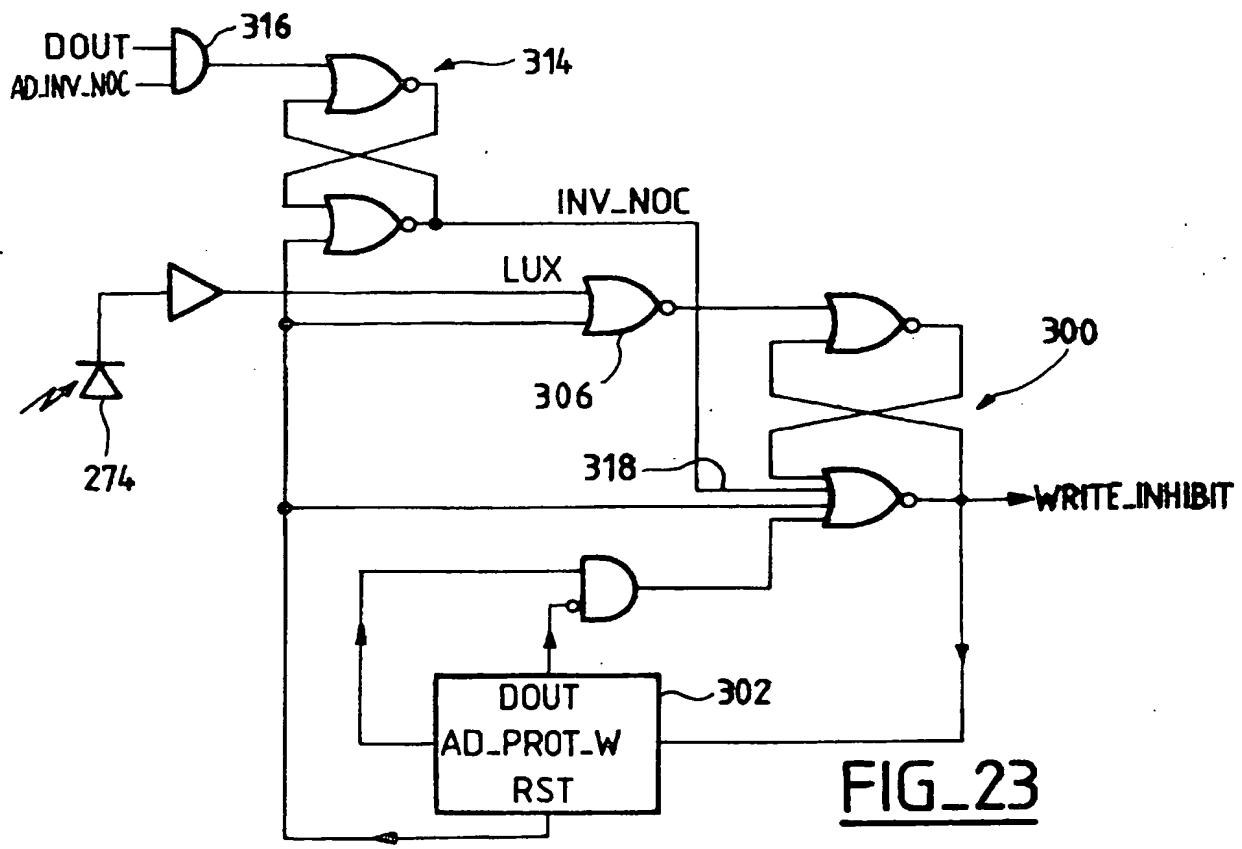
FIG_14

6/10

FIG_15FIG_16FIG_17FIG_18FIG_19

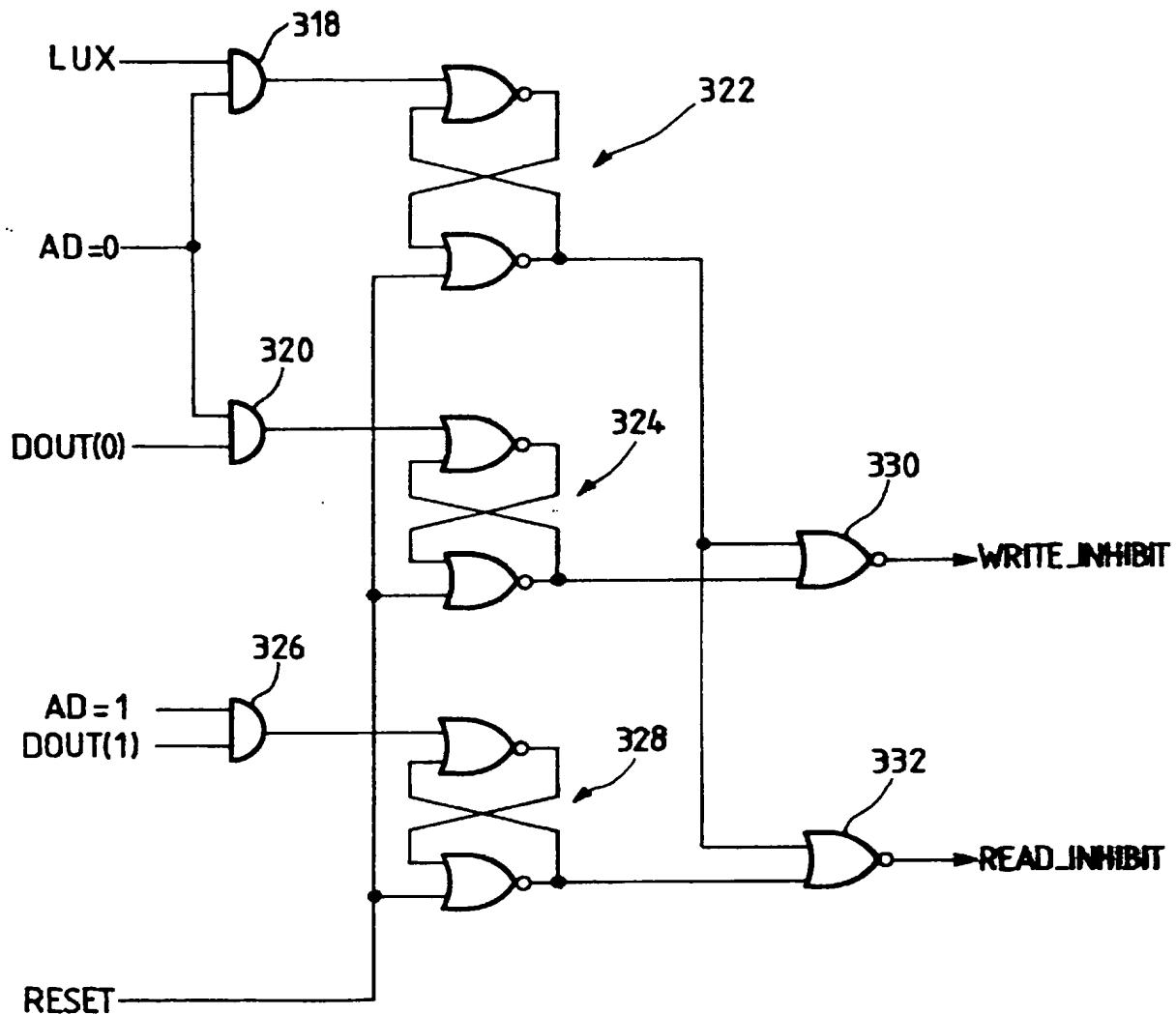
7/10

FIG_20FIG_21

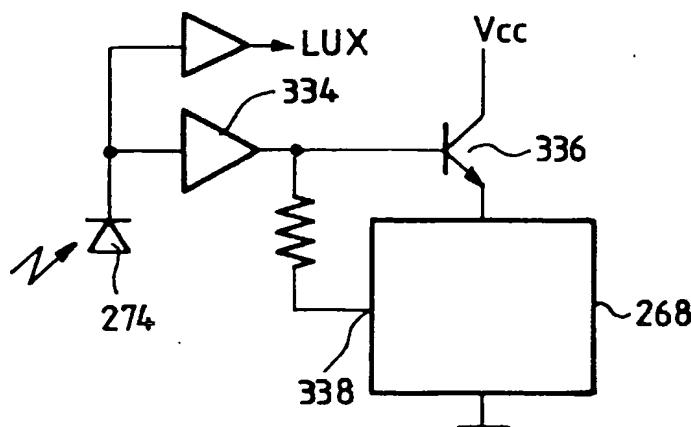
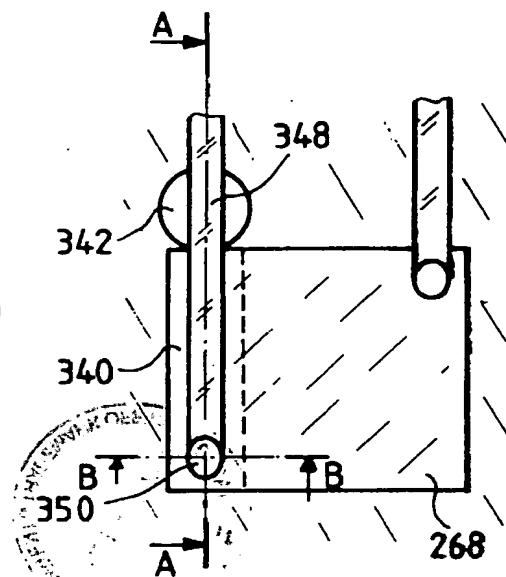
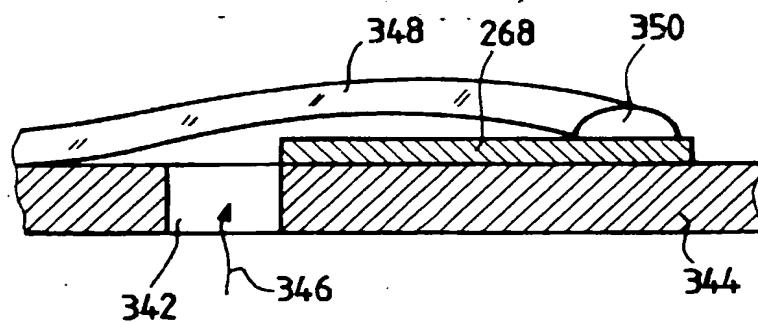
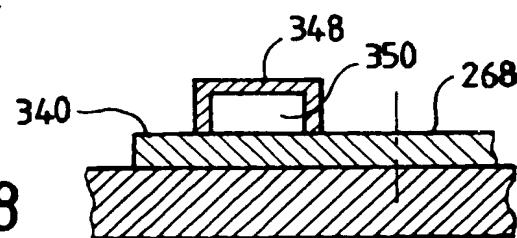
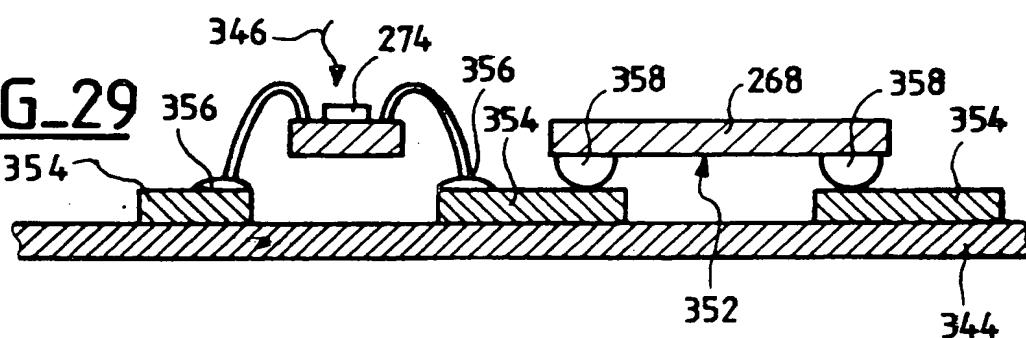
**FIG_22****FIG_23**

9/10

FIG_24



10/10

FIG_25FIG_26FIG_27FIG_28FIG_29

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE
PRELIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 555014
FR 9800428

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	GB 2 265 038 A (OLIVETTI RES LTD) 15 septembre 1993 * page 2, ligne 31 - ligne 34 * * page 3, ligne 10 - ligne 17 * * page 5, ligne 11 - ligne 13 * * revendications 4,6,7,16,18,20 * * ligne 11 - ligne 13 * ---	1,3,4
A	FR 2 665 008 A (ELGELEC) 24 janvier 1992 * revendication 1 * ---	1,3,4
A	FR 2 728 710 A (SOLAIC S.A.) 28 juin 1996 * revendication 1 * -----	1
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
G06K		
1	Date d'achèvement de la recherche 9 juillet 1998	Examinateur Herskovic, M
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>		